TRIBUTE TO MRS. OLLYE BALLARD CONLEY OF HUNTSVILLE, ALABAMA

HON. ROBERT E. "BUD" CRAMER, JR.

OF ALABAMA

IN THE HOUSE OF REPRESENTATIVES

Tuesday, July 10, 2001

Mr. CRAMER. Mr. Speaker, I rise today to honor Mrs. Ollye Ballard Conley on her June 30th retirement after more than 35 years of dedicated service to the Huntsville City school system. Mrs. Conley has made the students of the Huntsville community shine through her creation of a top-notch magnet school, the Academy for Science and Foreign Language.

Her career in education is extensive and very impressive. Beginning as a teacher in Limestone County, Mrs. Conley has spent time teaching in Germany with the Department of Defense as well. After returning to Huntsville, her career took off and she soon rose through the ranks to become an administrator and then principal. She has led the schools of University Place, Rolling Hills and most recently the Academy for Science and Foreign Language to be more efficient, better organized schools. She believes in mission and her mission has been to provide the best environment possible for children to excel. She is innovative bringing in new curriculums such as the National Service-Learning program. The Academy is the only middle school in Alabama and only one of 34 nationwide to implement the service-learning program. She has shared her knowledge and the benefits of the service-learning program as a Regional Trainer for the Southern Region Corporation for National Service-Exchange.

Mrs. Conley believes that an education does not have to be limited to the classroom. Along with her students whom she inspires to achieve more and give back to their community, she established the first annual Community Day at Glenwood cemetery earning the Huntsville Historical Society Award and the Alabama Historical Commission Distinguished Service Award.

On behalf of the United States Congress and the people of North Alabama, I want to personally thank Mrs. Conley and pay tribute to her for her being an unsung hero. The difference she has made in countless children's lives over the years is incalculable. I would like to extend my best wishes to her, her family, friends and colleagues as they celebrate her well-deserved rest and a job well done.

INTRODUCTION OF THE CYBER SECURITY INFORMATION ACT OF 2001

HON. TOM DAVIS

OF VIRGINIA

IN THE HOUSE OF REPRESENTATIVES

Tuesday, July 10, 2001

Mr. TOM DAVIS of Virginia. Mr. Speaker, I am pleased to rise today to reintroduce legislation with my good friend and colleague from northern Virginia, Representative, JIM MORAN. Last year, we introduced H.R. 4246 to facilitate the protection of our nation's critical infrastructure from cyber threats. We aggressively pushed forward with the legislation and held a productive Subcommittee hearing with the then-Subcommittee on Government Management, Information, and Technology on the importance of the bill. Based on comments made at that hearing, we have worked hard with a wide range of industries to refine and improve this legislation. Today, we are again introducing this legislation with the full partnership of the private sector. Over the past several months, I have worked with the industry leaders from each of our critical infrastructure sectors to draft consensus legislation that will facilitate public-private partnerships to promote information sharing to prevent our nation from being crippled by a cyber-terrorism threat.

In the 104th Congress, we called upon the previous Administration to study our nation's critical infrastructure vulnerabilities and to identify solutions to address these vulnerabilities. Through that effort, a number of steps were identified that must be taken in order to eliminate the potential for significant damage to our critical infrastructure. Foremost among these suggestions was the need to ensure coordination between the public and private sector representatives of critical infrastructure. The bill we are again introducing today is the first step in encouraging private sector cooperation and participation with the government to accomplish this objective.

Since early spring of this year, Congress has held a number of hearings examining the ability of our nation to cope with cyber security threats and attacks. For instance, the House Energy and Commerce has held numerous hearings regarding the vulnerability of specific Federal agencies and entities, and how those agencies are implementing—or not implementing—the appropriate risk management tools to deal with these threats. The House Judiciary Subcommittee on Crime has held a number of hearings specifically looking at cybercrime from both a private sector and a federal law enforcement perspective. These hearings have demonstrated the importance of better, more efficient information sharing in protecting against cyber-threats as is encompassed in the legislation I have introduced today.

Also, the National Security Telecommunications Advisory Committee (NSTAC) met in early June of this year to discuss the necessary legislative action to encourage industry to voluntarily work in concert with the federal government in assessing and protecting against cyber vulnerabilities. The bill I am introducing today was endorsed at the June meeting. In recent months, the Bush Administration has aggressively been working with industry to address our critical infrastructure protection needs and ensure that the federal government is better coordinating its' cybersecurity efforts. I look forward in the coming weeks to working with the Administration to enhance the public-private partnership that industry and government must have in order to truly protect our critical infrastructure.

The critical infrastructure of the United States is largely owned and operated by the private sector. Critical infrastructures are those systems that are essential to the minimum operations of the economy and government. Our critical infrastructure is comprised of the financial services, telecommunications, information technology, transportation, water systems, emergency services, electric power, gas and oil sectors in private industry as well as our National Defense, and Law Enforcement and International Security sectors within the government. Traditionally, these sectors operated largely independently of one another and coordinated with government to protect themselves against threats posed by traditional warfare. Today, these sectors must learn how to protect themselves against unconventional threats such as terrorist attacks, and cyber intrusions.

These sectors must also recognize the vulnerabilities they may face because of the tremendous technological progress we have made. As we learned when planning for the challenges presented by the Year 2000 rollover, many of our computer systems and networks are now interconnected and communicate with many other systems. With the many advances in information technology, many of our critical infrastructure sectors are linked to one another and face increased vulnerability to cyber threats. Technology interconnectivity increases the risk that problems affecting one system will also affect other connected systems. Computer networks can provide pathways among systems to gain unauthorized access to data and operations from outside locations if they are not carefully monitored and protected.

A cyber threat could quickly shutdown any one of our critical infrastructures and potentially cripple several sectors at one time. Nations around the world, including the United States, are currently training their military and intelligence personnel to carry out cyber attacks against other nations to quickly and efficiently cripple a nation's daily operations. Cyber attacks have moved beyond the mischievous teenager and are now being learned and used by terrorist organizations as the latest weapon in a nation's arsenal. During this past spring, around the anniversary of the U.S. bombing of the Chinese embassy in Belgrade, U.S. web sites were defaced by hackers, replacing existing content with pro-Chinese or anti-U.S. rhetoric. In addition, an Internet worm named ''Lion'' infected computers and installed distributed denial of service (DDOS) tools on various systems. An analysis of the Lion worm's source code revealed that it could send password files from the victim site to e-mail address located in China.

We have learned the inconveniences that may be caused by a cyber attack or unforeseen circumstance. Last year, many of individuals and companies were impacted by the ''I Love You'' virus as it moved rapidly around the world disrupting the daily operations of many of our industry sectors. The Love Bug showed the resourcefulness of many in the private sector in identifying and responding to such an attack but it amply demonstrated the weakness of the government's ability to handle such a virus. Shortly after the attack, Congress learned that the U.S. Department of Health and Human Services' (HHS) operating systems were so debilitated by the virus that it could not have responded adequately if we had faced a serious public health crisis at the same time. Additionally, the federal government was several hours behind industry in notifying agencies about the virus. If the private sector could share information with the government within a defined framework, federal agencies could have been made aware of the threat earlier on.

Last month, NIPC and FedCIRC received information on attempts to locate, obtain control of and plant new malicious code known as ''W32-Leaves.worm'' on computers previously